

Single Min-Entropy Random Source can be Amplified

Martin Plesch^{1,2} and Matej Pivoluska²

¹*Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia*

²*Faculty of Informatics, Masaryk University, Brno, Czech Republic*

Expansion and amplification of weak randomness with the help of untrusted quantum devices is a hot topic of current research. Here we contribute with a procedure for amplifying a single weak random source with the help of tri-partite GHZ-type entangled states. If the quality of the source measured in min-entropy rate reaches a fixed threshold $\log_2(\sqrt{3})$, perfect random bits can be produced. Presented procedure works well also on locally bit-fixing random sources, which cannot be characterized as Santha–Vazirani sources and thus using existing amplification procedures cannot be applied.

I. INTRODUCTION

In most cryptographic tasks, communicating parties rely on a random source which shall decide about a particular protocol being implemented. On the classical level no true randomness, i. e. independent uniformly distributed random bits, is available and production of pseudo-random sequences is based on assumptions on inaccessibility of certain information to the adversary, such as thermal noise of semiconductors or movement of mouse cursor of a computer user. In classical cryptography different techniques are used to tackle with such limited sources of randomness. Depending on the available resources, randomness extractors can either produce almost perfect randomness from a weak source and a short perfectly random key (so called *seed*), or they can use two (or more) independent weak random sources to produce a shorter, but almost perfect output (see [1] for a survey). Nevertheless in the most pessimistic adversarial scenario one is unable to rule out adversary's full knowledge of the underlying processes, because classical physical theories are deterministic.

With Quantum Protocols production of random numbers seems to be trivial, thanks to inherent randomness of quantum physics – measurement in a basis complementary to the basis in which the states were produced can guarantee a source of perfect randomness. Thus, if one can trust the devices used for randomness production, the task is theoretically trivial and experimentally feasible up to commercial applications [2].

One can, however, go a bit further and ask if the production of random numbers could be safe not only against an external adversary, but also towards the supplier of the device itself. The importance of this requirement is underlined by the experimental complexity and fragility of quantum devices, which practically prohibits direct testing of processes appearing within the device. Such security can be indeed achieved by using devices utilizing quantum states that exhibit super-classical correlation properties, which can be tested solely by processing input and output data. This check of the honesty of the devices, which is often performed simultaneously with the actual implemented protocol, is referred in a broader scope as Device Independence.

To design a Device Independent Random Number Generator, one can use the fact that states exhibiting super-classical correlations properties exhibit intrinsic randomness if measured locally. A line of research was devoted to expansion of free randomness using Quantum Devices (see e. g. [3–5]), which in the spirit of seeded randomness extractors, expands the length of preexisting independent random seed. Very recently several manuscript were published [6–10] suggesting ways to *amplify* existing weak randomness, i.e. creating independent random bits with the use of imperfect randomness and quantum correlations. In a related recent work [11] authors examine the minimal properties of random seed output needed to perform Bell tests. Some of these works consider even more general scenario, in which the adversary is only restricted by no-signaling. This can also be seen as an attempt to minimize the assumptions for which independent perfect randomness exists, since super-determinism can never be completely ruled out.

Within this paper we will contribute to the topic of production of perfect randomness with the use of untrusted quantum devices and a single weak source of available randomness. We will show that production of perfect random numbers is possible in a very simple and experimentally feasible scenario with a rather weak demand on the weak random source. We utilize three-partite GHZ-type entanglement, which leads to a possibility of distinguishing between classical and quantum states in one shot experiment, if perfect quantum devices are assumed. Contrary to most of the previous work [6, 8–10], here we characterize the weak source of randomness by its min-entropy rather than with a local probability bias. Such characterization assumes very little structure of the underlying probability distributions and allows for randomness production even in cases where no local limit can be imposed on bits of random source used.

The paper is organized as follows: In Section II we define the random production task in detail and state basic prerequisites. In Section III we define both min-entropy sources and Santha–Vazirani sources and discuss their difference, whereas in Section IV we present the main result and in Section V we conclude.

II. PREREQUISITES

Consider a following scenario: Alice would like to produce perfect random numbers. She asks her supplier, Eve, to supply a Random Number Generator (RNG). However, Alice does not really trust in Eve's honesty and would like to check that Eve really supplied a good RNG which fulfills two basic criteria:

- Bits provided are random. They have full entropy and there is no way to predict future bits by knowing settings of the RNG and bits produced in the past.
- Bits are free, they are not correlated to any other system, in particular not to a system owned by Eve.

On the other hand Eve would like to influence, or at least learn about the bits produced by the RNG. To do so, she is granted all power except the following limitations:

1. Alice's laboratory is safe towards tampering and any communication with outside world. This includes also impossibility of communication between RNG and Eve once RNG is delivered to Alice. This is a very natural limitation without which the whole task has no real sense, as if not fulfilled, the RNG could simply send the produced bits to Eve.
2. Alice can ask Eve to deliver RNG in parts. These parts can be prohibited to communicate within the laboratory among themselves. This can be viewed as a slight extension of the capability of Alice of isolating the laboratory towards outside world to her capability to isolate also parts of her lab among each other. As an alternative (though very impractical) this can be achieved by Alice working in a set of space-like separated labs, having a trusted agent in each part of the lab.
3. Eve is constrained by the laws of quantum mechanics. In particular any statistics achieved among parts of the RNG must obey relevant Tsirelson's bounds[12].
4. Alice has a source of somewhat random numbers. Apparently, if Alice has no such source, Eve could predetermine all steps of Alice in advance, simulate any results that Alice would expect and use to check honesty of Eve. The level of randomness of the source needed is a crucial parameter of the protocol and will be discussed later.

III. WEAK RANDOM SOURCES

We will model randomness Alice uses in her protocol by a random variable X . Alice's information about the probability distribution of X is $P(X)$, which might likely be a perfectly random distribution. We also assume that Eve has a random variable E with a probability distribution $P(E)$. Eve's information about X is given by the probability distribution $P(X|E)$ and can be viewed as

the level of correlation between the variables X and E . The only information we suppose about the distribution is that it is random at least to a certain extent; thus, we allow the output of X conditioned on E to be distributed according to any probability distribution containing sufficient randomness. The ultimate goal is then to design an algorithm, which can produce random outcome independent on E with inputs distributed according to a probability distribution $P(X|E)$.

We say that X conditioned on E contains some randomness if

$$P_g(X|E) = \sum_e P(E=e)P_g(X|E=e) < 1, \quad (1)$$

where $P_g(X|E=e) = \max_x P(X=x|E=e)$. This is equivalent to a condition that for at least one output e that Eve can receive with non-zero probability, she is unable to predict the output of Alice's random variable X with certainty.

We will quantify the amount of randomness of a distribution by its *min-entropy* defined by

$$H_\infty(X|E) = -\log_2 P_g(X|E). \quad (2)$$

A variable X is called an (N, b) -source with respect to E , if it emits N -bit strings drawn according to a probability distribution conditioned on E with a min-entropy of at least $b = H_\infty(X|E)$ bits. Thus, for every specific N -bit sequence $P_g(X|E)$ is smaller or equal to 2^{-b} . For $b = N$, one obtains a perfect source where all sequences are drawn with the same probability.

Let us denote here that an alternative definition of min-entropy reading

$$H_\infty^1(X|E) = -\log_2 \max_e P_g(X|E=e) \quad (3)$$

is also possible. Whereas the definition (2) deals with an average information Eve can obtain about X throughout many runs, single-run min-entropy (3) characterizes the maximum of information Eve can gain in a single run. As $H_\infty(X|E) \geq H_\infty^1(X|E)$ holds in general, and in particular the latter can be zero even if the earlier is non-zero, min-entropy defined by (2) is more relaxed measure assigning non-zero randomness to more sources. As the proposed protocol is designed for high number of runs and in particular is robust against single fixed bits on the raw output, use of (2) is perfectly suitable for characterizing the source and will allow more sources to be used for extraction.

We also define the *min-entropy rate*

$$R = \frac{H_\infty(X|E)}{N},$$

quantifying bits of entropy of the source per produced random bit. Min-entropy will be used as the figure of merit within this paper, characterizing the quality of random source used.

Here we shortly discuss a different definition of figure of merit of a random source, namely the so called Santha–Vazirani or S-V source introduced in [13]:

A string of random bit variables Z_i is a δ -SV source ($0 \leq \delta \leq \frac{1}{2}$) with respect to E if

$$\frac{1}{2} - \delta \leq P(Z_i = 0 | E, Z_1, \dots, Z_{i-1}) \leq \frac{1}{2} + \delta. \quad (4)$$

For $\delta = 0$ all Z_i are uniformly distributed and mutually independent and any randomness source, even completely deterministic one, can be described as a SV-source with $\delta = \frac{1}{2}$. Note that all possible distributions of N -bit strings distributed according to a SV-source, have min-entropy at least $-\log_2((\frac{1}{2} + \delta)^N)$ and the corresponding min-entropy rate $R \geq -\log_2(\frac{1}{2} + \delta)$. On the other hand, there are distributions with high min-entropy, which cannot be characterized as SV-sources with $\delta < \frac{1}{2}$. In particular a source with a single bit of the sequence fixed and all other bits perfectly random has min-entropy $H_\infty(X|E) = N - 1$ and thus $R \rightarrow 1$ for large N . Nevertheless, it can only be characterized as a SV-source with $\delta = \frac{1}{2}$.

This is due to the fact that SV-sources assume additional structure of the randomly distributed N -bit strings, namely that the influence of the adversary is limited locally (per bit) rather than a global limitation for min-entropy sources. This leads to a fact that amplification of SV sources is much easier in the sense that some amount of randomness is guaranteed to be present in each single bit from the random source. On the contrary, min-entropy sources guarantee only the global amount of randomness within the whole string and any protocol has to be robust especially against big-fixing source on the input.

In our work we put only minimal restrictions on the input random source in terms of min-entropy and due to this fact the proposed procedure can be utilized on a much broader class of sources than protocols previously known.

IV. AMPLIFICATION OF A WEAK MIN-ENTROPY SOURCE

Here we present a specific scenario that allows to utilize a rather weak random source for production of perfect random bits with the help of GHZ-type quantum correlations. We will work in a framework of noise-free quantum devices and sufficiently long keys.

Alice can formulate her order for Random Number Generator (RNG) to Eve in a following way:

1. RNG shall consist of three physically separable parties, Lucy, Julia and Gabriela.
2. Each party provides a single bit of output each time when it is supplied a single bit of input (we will denote the states of bits 1 and -1).

3. If all RNG parties are supplied by bit 1, the product of output bits shall be 1. If two parties of RNG are provided by -1 and one party by 1, the product of output bits shall be -1 . Any other input for the RNG is considered as ineligible.
4. The whole protocol will be aborted and the RNG will be returned if there is a single mistake in outputs of the devices. Eve, as a respected supplier, wants to be sure that this does not happen in any case.

It is straightforward to see that honest Eve can easily fulfill this task by sharing GHZ-like tripartite entangled states in the form

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \quad (5)$$

written in the z -basis, among parties of the RNG. Each party of the RNG will perform a measurement along x or y basis depending on the input bit and signal the result as the output. Each local measurement outcome will be perfectly random, as locally each party keeps a fully mixed state, but tri-partite entanglement among the parties guarantees proper product of outputs as expected.

Classically the correlations on output bits cannot be simulated. This can be viewed from the fact that if all outputs are predetermined, for 111 input zero or two parties must output a different bit than received, whereas for all other inputs one or three output bits have to be changed. This cannot be achieved locally without having information about the input. More interestingly, as it was proven in [3], GHZ-like states or superpositions thereof in higher dimensions are the only solution for this task in quantum domain. Thus, if Alice has free choice to select her input bits and Eve wants to be sure that she will not be detected and considered dishonest, she has to use a strategy that involves GHZ-like states and measurement in complementary bases.

Let us now analyze the flow of randomness within this protocol (supposing a source of perfect randomness owned by Alice). Alice shall choose randomly with the same probability one of following possibilities: either she sends to all three parties the bit 1, or one of the parties receives 1 and the others two -1 . To make her choice, Alice will use two bits of her randomness. It is easy to see that each party will receive 1 or -1 with 50% probability and by receiving a bit no party learns anything about the individual bits provided to other parties.

The output bits of each party are locally fully random, but are correlated across three RNG parties. Alice will use the bits produced by Gabriela for checking purposes (to see whether the product of bits produced corresponds to expectation) and will keep random bits produced by Lucy and Julia. Thus, for two bits of perfect input randomness Alice obtained two bits of perfect output. This procedure can be used to construct a randomness expansion device, when Alice will use a portion of the original

random key to remove correlations between input and output strings from RNG via privacy amplification.

Here we investigate a different scenario, where Alice has no perfect randomness, even in a limited amount. We will show that contrary to any classical processing, even from a single weak random source Alice can construct perfect random bits.

Let us now analyze strategies that Eve can apply if she can tamper the random source used by Alice in a single run of the experiment. We will divide Eve's strategies into two branches depending on the amount of information Eve can learn about the two bits used by Alice for selecting inputs for RNG:

1. Alice's source is "good enough" and all four possibilities have non-zero probability to appear.
2. The random source is so weak that Alice is prevented from choosing one of the possibilities such that no more than three of the possibilities appear with non-zero probability.

As proven by [3], in order to avoid any errors in output bits Eve has to use GHZ-like states and von-Neumann measurements in the RNG, if all possible inputs may appear with non-zero probability. This leads to perfectly random numbers on outcomes of the devices; we will denote this strategy as quantum in what follows.

On contrary, if only up to three combinations of input appear, parts of RNG can agree in advance on a classical strategy for producing output bits. If the combination 111 is ruled out for instance, each part of RNG can reply a negation of the input bit, or they can even agree that one of them will deterministically output bit -1 and the others 1. Strategy can be varied from run to run such that Alice will not be able to detect any regularity in the output bits.

The crucial aspect here is the fact that whatever strategy is chosen by the parts of the RNG, it had to be agreed collectively in advance (before the device was delivered to Alice) and the strategy can in particular not depend on the output of previous experiments performed by parts of the RNG. Thus, each part of the RNG has to know in advance, whether a classical or quantum strategy will be chosen for a specific run and if a classical strategy is chosen, how to produce the output bit. These bits might be predetermined or depend on the input bits for the specific run, but cannot depend on bits produced before with the quantum strategy. Thus bits produced with use of classical strategy might have zero entropy, but will not be correlated with any bits previously produced using quantum strategy.

To completely avoid one of the four possibilities of choice for Alice, the probability of the remaining three options has to be at least as large as $\frac{1}{3}$. Thus, if the two random bits used by Alice have min-entropy larger than $\log_2(3)$, the first option would arise and Eve has to implement the quantum strategy, otherwise she can apply the classical one.

Extending this to more runs, output of all runs can be fully predetermined by Eve only if the min-entropy of the source does not exceed $N \log_2(3)$. Thus, if the min-entropy rate of Alice's weak random source is at most

$$R_{\max} = \log_2(\sqrt{3}), \quad (6)$$

Eve will be able in every single run of the experiment rule out one of the possibilities of choice and implement the classical strategy. In such a case the resulting bits are not random at all and could have been prepared well in advance by Eve. Thus, Alice will not gain any further randomness and will also not be able to distinguish a completely classical strategy used by Eve from the expected quantum one. Interestingly, this rate exactly corresponds to the minimal min-entropy needed to be able to draw any conclusions about the outcomes of any Bell test [11].

On the other hand, if the min-entropy rate is larger than R_{\max} , Eve will not be able to apply the classical strategy in all runs. In some of the runs Eve will not be able to rule out one of the four possibilities of input for RNG and she has to use quantum strategy to prevent Alice from detecting an error. As quantum strategy leads inherently to perfect randomness on the output, the final output string produced by both Lucy and Julia will independently have following properties:

1. Each bit in the output string was produced either by quantum or classical strategy; there is at least one bit produced by quantum strategy in the output string.
2. Each bit produced by quantum strategy is perfectly random and not correlated to any previous input or output.
3. Each bit produced by classical strategy may be either completely predetermined, or may depend on the input bit of the specific run. But it may not depend on any of the bits produced by quantum strategy.

Min-entropy of the output string is non-zero, as it is partially random, but it might be arbitrary low if $R \rightarrow R_{\max}$. It contains no randomness if we view it as a SV-source, as some of the bits can be predetermined and thus $\delta = \frac{1}{2}$.

Yet it is very easy to extract a single bit of randomness from this string due to the lack of correlations between the bits produced with different strategies. As the "classically" produced bits cannot depend on the bits produced by quantum strategy, it is sufficient to make a product of all bits of the string to produce a single perfect random bit, as a product of a single random bit with anything not correlated to this bit yields a perfect random bit again. Thus, in spite of the fact that the string of bits produced is very weakly random in the standard measures of randomness, its specific correlation properties allow simple extraction of randomness from it.

Before we finalize, let us briefly discuss any other possible strategies Eve may apply to tamper the protocol. One could think about using more dimensions, complex entangled states across all the runs of the experiment as well as more complicated POVMs with classical post-processing of data etc. All these strategies can be divided into two basic groups. The first group consist of strategies involving a GHZ state and von-Neumann measurements in complementary bases, as well as combination of GHZ states on higher dimensional systems with suitable two-outcome partial measurements. Due to [3] these are the only states that can provide error-free correlation outcomes as expected by Alice. They all have the same output statistics and there is no way of discrimination between these strategies only by input/output statistics, so they can be all subsumed under the "quantum" strategy.

All other strategies form the second group. Strategies in this group have a non-zero probability of error in the outcome for at least one of the four inputs and thus can be used only if Eve can guarantee that one of the input options will be ruled out. These strategies may produce almost any bits in the outcome, however independently on outcomes of strategies from the first group. There is no way how to discriminate any of these strategies from the "classical" strategy only by input/output statistics. Therefore we can subsume all these strategies under "classical" strategy as described above.

V. CONCLUSION

We have presented a scheme for production of perfect random numbers with untrusted quantum devices and a single weak random source, based on tri-partite GHZ-type entanglement. This scheme can be used for production of perfect randomness by parallel monitoring the honesty of the devices. We use min-entropy to characterize the randomness of the source, which guar-

antees the minimal possible assumptions about its detail characteristics, in particular about any local behavior. This allows amplification of a wide variety of weak random sources including sources not amplifiable by already known procedures.

Perfection of the randomness produced is obtained under the assumption of perfect quantum devices, so that no errors whatsoever are tolerated in the outputs. As the suggested scheme is routinely realizable in laboratory conditions particularly on photons, one might be interested in the question as how the situation changes for real conditions, where one has to accept that even a honest device supplied by Eve will with some probability supply an incorrect output. To tackle with this fact, one has to accept that with some probability, RNG will output results that do not fulfill conditions stated in the previous section. This naturally and unavoidably leads to a back-door for Eve - if she can produce better devices than she claims, she might use the rest of tolerated errors to tamper the randomness produced. Here Alice has to use a more complicated post-processing strategy to prevent Julia and Lucy from choosing locally a suitable bit in the last run and fixing therewith the product, risking a 50% probability of error. Based on our ongoing work and numerical research we conjecture that the bias in the probability of the output random bit will be bounded by $O\left(\sqrt{\frac{4^R p}{4^R - 3}}\right)$ with p the tolerated probability of an error in the output and R the min-entropy rate of the source.

VI. ACKNOWLEDGEMENT

We acknowledge the support of the Czech Science Foundation GACR project P202/12/1142, as well as project VEGA 2/0072/12.

-
- [1] R. Shaltiel. Bulletin of the European Association for Theoretical Computer Science, 77:6795, (2002)
 - [2] See e.g. <http://www.idquantique.com/component/content/article.html?id=9>
 - [3] R. Colbeck and A. Kent, J. Phys. A: Math. Theor. 44, 095305 (2011)
 - [4] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Nature 464, 1021 (2010)
 - [5] U. Vazirani and T. Vidick, arXiv:1111.6054v1 (2011)
 - [6] R. Colbeck and R. Renner, Nature Physics 8, 450-454 (2012)
 - [7] D. E. Koh, M. J. W. Hall, Setiawan, J. E. Pope, C. Marletto, A. Kay, V. Scarani, A. Ekert, Phys. Rev. Lett. 109, 160404 (2012)
 - [8] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, A. Acin, arXiv:1210.6514 (2012)
 - [9] P. Mironowicz, M. Pawlowski, arXiv:1301.7722 (2013)
 - [10] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawlowski, R. Ramanathan, arXiv:1303.5591 (2013)
 - [11] L. P. Thinh, L. Sheridan, V. Scarani, arXiv:1304.3598, (2013)
 - [12] B. S. Cirel'son, Lett. Math. Phys. 4, 93 (1980)
 - [13] M. Santha and U. V. Vazirani. Journal of Computer and System Sciences, 33:75, (1984)